(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－148014
（P2000－148014A）
(43)公開日　平成12年５月26日(2000.5.26)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｂ０５７
Ｇ０６Ｔ　1/00		Ｈ０４Ｎ　1/387		５Ｃ０７６
Ｈ０４Ｎ　1/387		Ｇ０６Ｆ　15/66	Ｂ	５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全５頁）

(21)出願番号　特願平10－321887

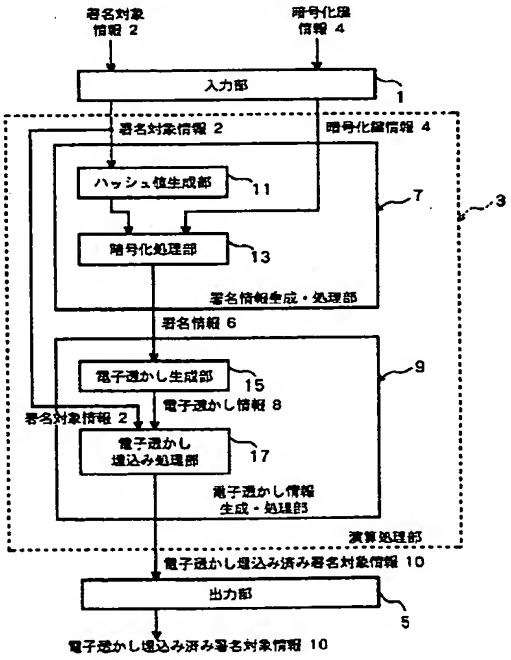
(22)出願日　平成10年11月12日(1998.11.12)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　林　誠一郎
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095371
弁理士　上村　輝之

Ｆターム(参考)　5B057 AA20 CA12 CA16 CA18 CB12
CB16 CB18 CC01 CE08 CG07
5C076 AA14 BA06
5J104 AA14 AA15 JA28 MA02 NA12
NA15 PA14

(54)【発明の名称】　電子署名情報付与方法及び装置

(57)【要約】
【課題】　第三者による署名者本人の成りすましを防止できるようにする。
【解決手段】　電子透かし生成部１５では、暗号化処理部１３からの署名情報６を読込み、その各桁毎の意味付けに基づき、署名情報６の電子透かし情報８を生成する。電子透かし埋込み処理部１７では、透かし情報８を読込んで入力部１からの署名対象情報２に埋込むことにより、電子透かし埋込み済み署名対象情報１０を作成する。透かし情報８の対象情報２への埋込みは、例えばＤＣＴ法及びＩＤＣＴ法を用いて行われる。対象情報２から署名情報６が容易に読出されたり、分離されたり、別の署名情報が対象情報２に不正に付加されたりするのを防止するため、埋込み処理部１７において、透かし情報８が対象情報２の複数箇所に分散して埋込まれる。透かし情報８は埋込み処理部１７によって対象情報２中の不規則に決められた複数の箇所に夫々埋込まれる。第三者による署名者本人の成りすましをより確実に防止することが可能になる。



1

【特許請求の範囲】

【請求項１】　与えられた電子署名情報に基づいて、その透かし情報を生成する手段と、

前記透かし情報を、与えられた署名対象情報の複数箇所に埋込む手段と、

を備える電子署名情報付与装置。

【請求項２】　請求項１記載の電子署名情報付与装置において、

前記埋込み手段が、前記透かし情報を、前記署名対象情報中の不規則に決めた複数箇所に埋込むことを特徴とする電子署名情報付与装置。

【請求項３】　請求項１記載の電子署名情報付与装置において、

前記透かし情報の生成が、離散コサイン変換法を用いて行われ、前記透かし情報の埋込みが、離散コサイン変換法及び逆離散コサイン変換法を用いて行われることを特徴とする電子署名情報付与装置。

【請求項４】　請求項１記載の電子署名情報付与装置において、

前記電子署名情報が、ハッシュ化された前記署名対象情報に、前記署名対象情報の著作者の秘密鍵で暗号化処理を施されて生成されることを特徴とする電子署名情報付与装置。

【請求項５】　請求項４記載の電子署名情報付与装置において、

前記暗号化処理が、ＲＳＡ公開鍵暗号方式を用いて行われることを特徴とする電子署名情報付与装置。

【請求項６】　与えられた電子署名情報に基づいて、その透かし情報を生成する第１の過程と、

前記透かし情報を、与えられた署名対象情報の複数箇所に埋込む第２の過程と、

を備える電子署名情報付与方法。

【請求項７】　与えられた電子署名情報に基づいて、その透かし情報を生成する手段と、

前記透かし情報を、与えられた署名対象情報の複数箇所に埋込む手段と、

を備える電子署名情報付与装置における前記各手段としてコンピュータを動作させるためのコンピュータプログラムを担持したコンピュータ読取可能なプログラム媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子署名情報付与方法及び電子署名情報付与装置の改良に関するものである。

【０００２】

【従来の技術】従来、画像情報や音声情報等の著作者は、それらの著作物を署名対象情報として自身の電子署名情報を付加し、保管又は相手方端末への送信等を行っている。

2

【０００３】

【発明が解決しようとする課題】ところで、上記方法では、上記電子署名情報が上記署名対象情報に単に付加されているだけであるので、第三者が署名者本人に成りすまし、署名者本人が有する秘密鍵とは別の秘密鍵で新たな電子署名情報を不正に作成して上記署名対象情報に付加することが容易に行える。そのため、上記方法では、上記成りすましを防止する手段として、第三者機関である認証局の発行する証明書により、上記署名対象情報への署名者が本人であるか否かの確認に対して信頼性を持たせる必要があった。

【０００４】従って本発明の目的は、第三者による署名者本人の成りすましを防止することができるようにすることにある。

【０００５】

【課題を解決するための手段】本発明の第１の側面に従う電子署名情報付与装置は、与えられた電子署名情報に基づいて、その透かし情報を生成する手段と、その透かし情報を、与えられた署名対象情報の複数箇所に埋込む手段とを備える。

【０００６】上記構成によれば、電子署名情報の透かし情報が、与えられた署名対象情報の複数箇所に埋込まれるので、第三者機関である認証局の発行する証明書により、上記署名対象情報への署名者が本人であるか否かの確認を行わなくても、第三者による署名者本人の成りすましを防止することができる。

【０００７】本発明の第１の側面に係る好適な実施形態では、透かし情報が、埋込み手段によって署名対象情報中の不規則に決めた複数箇所に埋込まれる。そのため、第三者による署名者本人の成りすましをより確実に防止することができる。

【０００８】上述した透かし情報の生成は、例えば離散コサイン変換法を用いて行われ、また、上記透かし情報の埋込みは、例えば離散コサイン変換法及び逆離散コサイン変換法を用いて行われる。また、上記の電子署名情報は、ハッシュ化された署名対象情報に、署名対象情報の著作者の秘密鍵で暗号化処理を施されて生成される。この暗号化処理は、ＲＳＡ（リベストーシャミールーアドルマン）公開鍵暗号方式を用いて行われる。なお、署名対象情報のハッシュ化により、上記署名対象情報に対する演算処理速度が高速化される。

【０００９】本発明の第２の側面に従う電子署名情報付与方法は、与えられた電子署名情報に基づいて、その透かし情報を生成する第１の過程と、その透かし情報を、与えられた署名対象情報の複数箇所に埋込む第２の過程とを備える。

【００１０】本発明の第３の側面に従うプログラム媒体は、与えられた電子署名情報に基づいて、その透かし情報を生成する手段と、その透かし情報を、与えられた署名対象情報の複数箇所に埋込む手段とを備える電子署名

情報付与装置における上述した各手段としてコンピュータを動作させるためのコンピュータプログラムをコンピュータ読取可能に担持する。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１２】図１は、本発明の一実施形態に係る電子署名情報付与装置の全体構成を示すブロック図である。

【００１３】上記装置は、図１に示すように、入力部１と、演算処理部３と、出力部５とを備える。

【００１４】入力部１には、署名対象情報（つまり、電子署名情報の付与対象になる情報）２として、例えば絵画等の画像情報、文学作品等のテキスト情報、及び楽譜等の著作物や、その他の諸情報が入力される。入力部１には、また、上記署名対象情報に、それらの著作者の電子署名情報を付与するために用いる上記著作者の暗号化鍵情報（上記著作者自身の秘密鍵情報）４も入力される。上述した署名対象情報２及び暗号化鍵情報４は、演算処理部３によって適宜読込まれる。

【００１５】演算処理部３は、機能的に見て署名情報生成・処理部（生成・処理部）７と、電子透かし情報生成・処理部（生成・処理部）９とに大きく区分される。更に、生成・処理部７は、ハッシュ値生成部１１と、暗号化処理部１３とに区分され、一方、生成・処理部９は、電子透かし生成部（透かし生成部）１５と、電子透かし埋込み処理部（埋込み処理部）１７とに区分される。

【００１６】ハッシュ値生成部１１は、入力部１からの署名対象情報２を読込んで、それにハッシュ関数（データ圧縮型スクランブル処理）を施すことにより上記署名対象情報２のハッシュ値を生成し（つまり、上記署名対象情報２をハッシュ化し）、暗号化処理部１３に出力する。ここで、ハッシュ関数とは、任意の長さの平文を特定の長さに変換（つまり、圧縮）する関数で、変換された結果から元の平文への変換（つまり、逆方向への変換）が容易に行えない一方向性関数である。ハッシュ値生成部１１において、上記署名対象情報２をハッシュ化する理由は、演算処理部３における上記署名対象情報２に対する演算処理速度を高速化するためである。

【００１７】暗号化処理部１３は、入力部１からの暗号化鍵情報４を読込んで、例えばＲＳＡ（リベストーシャミールーアドルマン）公開鍵暗号方式により、ハッシュ値生成部１１からのハッシュ化された上記署名対象情報２を暗号化処理する。この暗号化処理により、上記署名対象情報２から「１」及び「０」の２個の数を用いて複数桁の２値化情報（ディジタル情報）として表現される上記著作者の署名情報６が生成される。上記生成処理において、例えば、上記署名情報６を構成する各桁のうち、奇数の値をとる桁については「１」が、偶数の値をとる桁については「０」が、夫々付与されることにより、各桁毎に夫々意味付けが行われる。この署名情報６は、暗号化処理部１３から透かし生成部１５に出力される。

【００１８】透かし生成部１５では、暗号化処理部１３からの上記署名情報６を読込んで、上述した各桁毎の意味付けに基づき、上記２値化情報から上記署名情報６の電子透かし情報８を生成する。この電子透かし情報８は、通常、各種の連続的な物理量により表現される情報、即ち、例えば著作者のＩＤ情報やロゴ・マーク等のアナログ情報として示される。

【００１９】例えば、電子透かし情報８の署名対象情報２への埋込みを、ＤＣＴ法（離散コサイン変換法）及びＩＤＣＴ法（逆離散コサイン変換法）を用いて行うときは、署名対象情報２に周波数変換の手法を施すことにより署名対象情報２から得られる各周波数成分毎の振幅の大きさに対応する値が、上記署名情報６に該当する。なお、ＤＣＴ法における周波数変換の手法は、上記署名対象情報２が音声情報である場合には勿論のこと、上記署名対象情報２が静止画や動画等の画像情報である場合でも、その画像情報を構成する各画素毎の輝度の相違を波形と見做すことで適用が可能である。上記電子透かし情報８は、透かし生成部１５から埋込み処理部１７に出力される。

【００２０】埋込み処理部１７では、透かし生成部１５からの上記電子透かし情報８を読込んで入力部１からの署名対象情報２に埋込むことにより、電子透かし埋込み済み署名対象情報（埋込済み情報）１０を作成する。電子透かし情報８の署名対象情報２への埋込みは、例えば上述したＤＣＴ法及びＩＤＣＴ法を用いて行われる。ここで、上記署名対象情報２が画像情報である場合には、上述したように、その画像情報を構成する各画素毎の輝度の相違を波形と見做すことで周波数変換の手法を適用して原画像を示す周波数帯域及び振幅領域中から、可視画像を示す周波数帯域及び振幅領域を抽出する。次に、上記原画像領域から上記可視画像領域を除いた領域中の、予め決められた複数の周波数成分に対応する箇所に、上記電子透かし情報８を構成する複数個の波形を夫々埋込むと共に画像圧縮を行った後、更に、ＩＤＣＴ法を用いて元の画像情報に戻す。

【００２１】これにより、上記電子透かし情報８が人間に気付かれない程度にごく僅かなノイズとなって埋込まれた画像情報が、上記埋込済み情報１０として作成される。上記署名対象情報２が音声情報である場合には、勿論、上述したＤＣＴ法及びＩＤＣＴ法を用いて上記電子透かし情報８の埋込みが行われ、上記埋込済み情報１０が作成される。

【００２２】更に、本実施形態では、署名対象情報２から署名情報６が容易に読出されたり、分離されたり、或いは、別の署名情報が署名対象情報２に不正に付加されたりするのを防止するため、埋込み処理部１７において、電子透かし情報８が、署名対象情報２中の不規則に

決められた複数の箇所に分散して夫々埋込まれる。これにより、第三者による署名者本人の成りすましをより確実に防止することが可能になる。

【００２３】なお、上記埋込済み情報１０は、上記埋込み処理部１７から出力部５を通じて記憶部（図示しない）に出力され、記憶部（図示しない）に保存される他、ネットワーク（図示しない）等を通じて相手方端末（図示しない）へと送信される。

【００２４】図２は、上述した生成・処理部７における署名情報生成の処理動作、及び生成・処理部９における電子透かし情報生成の処理動作を示すフローチャートである。

【００２５】図２において、まず、生成・処理部７で、署名対象情報２と暗号化鍵情報４とに基づき、署名対象情報２に付与するための署名情報６が生成される（ステップＳ２１）。次に、生成・処理部９の透かし生成部１５で、上記署名情報６の電子透かし情報８が生成される（ステップＳ２２）。その後、その電子透かし情報８が、埋込み処理部１７で署名対象情報２の不規則に決められた複数の箇所に分散して埋込まれることにより、電子透かし埋込み済み署名対象情報１０が作成される（ステップＳ２３）。

【００２６】図３は、上述した生成・処理部７における署名情報生成の処理動作の詳細を示すフローチャートである。

【００２７】図３において、まず、ハッシュ値生成部１１で、読込んだ署名対象情報２がハッシュ化され（ステップＳ２４）、次に、暗号化処理部１３で暗号化鍵情報４に基づいて、ハッシュ化された上記署名対象情報２が暗号化処理され、それにより、署名情報６が生成される（ステップＳ２５）。そして、その署名情報６が生成・処理部９の透かし生成部１５に出力されることになる。

【００２８】以上説明したように、本発明の一実施形態によれば、署名情報６の電子透かし情報８が、署名対象＊情報２中の不規則に決められた複数の箇所に分散して夫々埋込まれる。そのため、従来のような、署名情報が単に署名対象情報に付加されているだけの場合と異なり、署名対象情報２から署名情報６が容易に読出されたり、分離されたりする不具合を防止できる。また、第三者が署名者本人に成りすまし、署名者本人が有する秘密鍵とは別の秘密鍵で新たな電子署名情報を不正に作成して上記署名対象情報２に付加したりするような不具合も確実に防止することができる。

【００２９】上述した内容は、あくまで本発明の一実施形態に関するものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。

【００３０】

【発明の効果】以上説明したように、本発明によれば、第三者による署名者本人の成りすましを防止するようにすることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る電子署名情報付与装置の全体構成を示すブロック図。

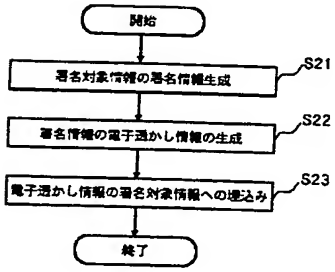
【図２】図１の署名情報生成・処理部の署名情報生成の処理動作、及び電子透かし情報生成・処理部の電子透かし情報生成の処理動作を示すフローチャート。

【図３】図２の署名情報生成の処理動作の詳細を示すフローチャート。

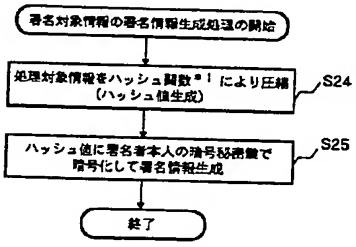
【符号の説明】

１　入力部
３　演算処理部
５　出力部
７　署名情報生成・処理部（生成・処理部）
９　電子透かし情報生成・処理部（生成・処理部）
１１　ハッシュ値生成部
１３　暗号化処理部
１５　電子透かし生成部（透かし生成部）
１７　電子透かし埋込み処理部（埋込み処理部）

【図２】



【図３】



【図１】